REMARKS

Claim 12 has been amended. No new matter has been added. Claims 8 to 18 are now pending. Applicants respectfully request reconsideration of the present application in view of this Response.

Applicants thank the Examiner for indicating that the Drawings have been accepted

35 U.S.C. §112, first paragraph

Claim 12 was rejected under 35 U.S.C. §112, first paragraph, for lack of written description. Applicants respectfully submit that claim 12 as written was supported by the Specification. For example, see Fig 4 and accompanying text which indicate that crypto-hardware is to be used. Notwithstanding, Applicants amended claim 12 so as to convey that the external crypto-hardware may include a chipcard and other hardware.et al. Accordingly, Applicants respectfully submit that claim 12 as presented is fully supported by the written description in the Specification, and withdrawal of the rejection under 35 U.S.C. §112, first paragraph, is respectfully requested.

35 U.S.C. §103

Claims 8 and 18 were rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Patent No. 5,805,204 to Thompson ("Thompson reference") in view of U.S. Patent No. 6,285,991 to Powar ("Powar reference").

The Thompson reference refers to an interactive video guide in which object code is transmitted to set-top decoder units located in customers' homes. The Thompson reference at col. 7, describes an interactive video display, data system head end computer and decoder which may incorporate smart card interfaces which will allow smart cards with imbedded keys to be able to be used to encrypt data before it is transmitted over the system and decrypt the data after it is received at the subscriber unit. The reference further indicates that to send encrypted data, a random number is first generated by a program within the headend computer; and an appropriate imbedded key (the chosen key for the time period) is selected and loaded into the system specific algorithm (which can be DES). The random number is encrypted using the DES algorithm which has been initialized and loaded with the appropriate key, producing a result which is the current system seed key. The seed key is then loaded into the system specific algorithm (i.e., polynomial generator) through which the actual transmitted data is passed. The initial random number is transmitted in clear text along with the encrypted data. When the data is received by a subscriber unit, a period identifier (i.e., date) may be used to identify which of the keys previously and securely imbedded into the smart card will be used for the decryption process. This key must be the same one used at the headend computer for the same time period.

The Powar reference refers to an interactive electronic account statement delivery system for using over the Internet. The Powar reference refers to a system where the certification authority grants digital certificates to the certificated banks, which in turn grant digital certificates to billers and customers. Then, digital certificates form the basis for encryption and authentication of network communications, using public and private keys. The reference refers to the certificates as being stored as digital data on storage media of a customer's or biller's computer system, or contained in integrated circuit or chip cards physically issued to billers and customers. Further, the reference recites that the electronic bill itself may be a simple text message, or may contain a number of embedded links, for example an embedded URL of a biller's world wide web server that allows the customer to interactively bring up detailed billing information by activating the link.

In contrast, claim 8 is directed to a method for implementing an encryption system, including generating a Vernam key via a symmetrical cipher, the generating being aided by using a secret key and a variable parameter, the Vernam key having a length that is equal to a length of a message to be protected, the secret key having a defined key length, the variable parameter having a length which is a function of the defined key length; encrypting, via a Vernam key, the message using logic operations of a Vernam cipher; communicating, from a sending point to a receiving point, the secret key and the variable parameter via at least one of (A) a secure channel separate from a message-transmission path and (B) the message-transmission path, the message-transmission path being secured via an asymmetrical cipher; regenerating the Vernam key; decrypting the message using the regenerated Vernam key; installing a storage space and one of a symmetrical cipher and the asymmetrical cipher in a crypto-module, the crypto-module being separate from an encryptor; and performing encryption operations via the Vernam cipher in the encryptor.

Neither of the references, alone or in combination, appear to teach or describe a Vernam key which is regenerated, or installing a storage space and one of a symmetrial cipher and an asymmetrical cipher in a crypto-module, the crypto-module being separate from the encryptor, and performing encryption operations via the Veranm ciper in the encryptor. Further, Applicants respectfully submit that the references are not combinable as one reference concerns itself with set-top devices which receive signals and the other reference concerns itself with an account delivery system, each of the systems concerning a different transmission of confidential information.

Accordingly, Applicants respectfully submit that the Thompson and Powar references in combination or alone do not teach or describe all of the features of claim 8. Allowance of claim 8 is respectfully requested. Further, since claims 9 to 17 depend from claim 8, those claims should be allowable for at least the same reasons as claim 8. And, claim 18 recites features

analogous to those of claim 8, and should be allowable for essentially the same reasons as claim 8.

Accordingly, Applicants respectfully request withdrawal of the rejection under 35 U.S.C. § 103(a) over the Thompson reference in view of the Powar reference.

CONCLUSION

For at least the foregoing reasons, Applicants respectfully submit that any outstanding rejections of claims 8 to 18 under 35 U.S.C. §§ 103(a), 112 have been overcome, and that those claims are allowable. It is therefore respectfully requested that the rejections be reconsidered and withdrawn, and that the present application issue as early as possible.

Respectfully submitted,

Dated: Monday, December 29, 2008

By: /Linda Lecomte/_____
Linda Shudy Lecomte (Reg. No. 47,084)

CUSTOMER NO. 26646

KENYON & KENYON LLP
One Broadway
New York, New York 10004
(212) 425-7200